Supply Chain Integrity, Transparency, and Trust (SCITT)

IETF#114 WG Forming BoF

28 July 2022

Note Well

- Any submission to the IETF intended by the Contributor for publication as all or part of an IETF Internet-Draft or RFC and any statement made within the context of an IETF activity is considered an "IETF Contribution". Such statements include oral statements in IETF sessions, as well as written and electronic communications made at any time or place, which are addressed to:
  - The IETF plenary session
  - The IESG, or any member thereof on behalf of the IESG
  - Any IETF mailing list, including the IETF list itself, any working group or design team list, or any other list functioning under IETF auspices
  - Any IETF working group or portion thereof
  - Any Birds of a Feather (BOF) session
  - The IAB or any member thereof on behalf of the IAB
  - The RFC Editor or the Internet-Drafts function
- All IETF Contributions are subject to the rules of RFC 5378 and RFC 8179.
- Statements made outside of an IETF session, mailing list or other function, that are clearly not intended to be input to an IETF activity, group or function, are not IETF Contributions in the context of this notice. Please consult RFC 5378 and RFC 8179 for details.
- A participant in any IETF activity is deemed to accept all IETF rules of process, as documented in Best Current Practices RFCs and IESG Statements.
- A participant in any IETF activity acknowledges that written, audio and video records of meetings may be made and may be available to the public.

Agenda

- Welcome and Introduction (5 min): Chairs
- BoF Goals and Interim BoF Recap (5 min): Chairs
- Problem Statement (10 min): Robert Martin (MITRE)
- Terms & Architecture (15 min): Cedric Fournet (Microsoft)
- Clarifying Questions (5 min)
- Milestones & Program of Work (10 min): Henk Birkholz (Fraunhofer SIT)
- Discussion (50 min): Everyone
- BoF Questions (15 min): Chairs / Area Director
- Wrap-up and Conclusion (5 min): Area Director

Interim BoF Recap

- Virtual BoF held on 16 June 2022
- Notes available at:

https://notes.ietf.org/notes-ietf-interim-2022-scitt-01-scitt

- The Software Supply Chain use case was detailed
- Good participation
- Results
  - AGREEMENT: problem statement
  - QUESTIONS: deliverables and the solution space

Post Interim BoF Implementation “Commitment”

https://mailarchive.ietf.org/arch/msg/scitt/FJOQMXS4i8-iJMerfn8KQDPNckQ/

Replies to “[i]f you plan to work on implementations” …

Software Supply Chain Use Case

- Arm
- Cloudflare
- Microsoft
- Reversing Labs
- MITRE
- Transmute
- Reliable Energy Analytics
- Mesur.io

Other Use Cases

- Mesur.io
- Transmute
- RKVST
- Telefonica
- Citizen's Oversight Project
- Arm

BoF Goals

Bringing relevant stakeholders into the room

Elicit feedback and assess consensus on:

- Working on this problem statement in the IETF
- Approach responsive to diversity of interest
  - Explicitly (proposed) charter scope around “software supply chain” use case
  - Generic framing of terminology, architecture, roles to maximize reuse
- Scope of solution and deliverables (see proposed charter)
  - https://github.com/ietf-scitt/charter/blob/master/ietf-scitt-charter.md
- Gauge degree of support to form a WG

Problem Statement

Problem Statement

Software is an inherent part of everyday digitally-enabled life, from smartphones to IoT to datacenters. Widely discussed attacks on the software supply chain have helped raise awareness of the risks.

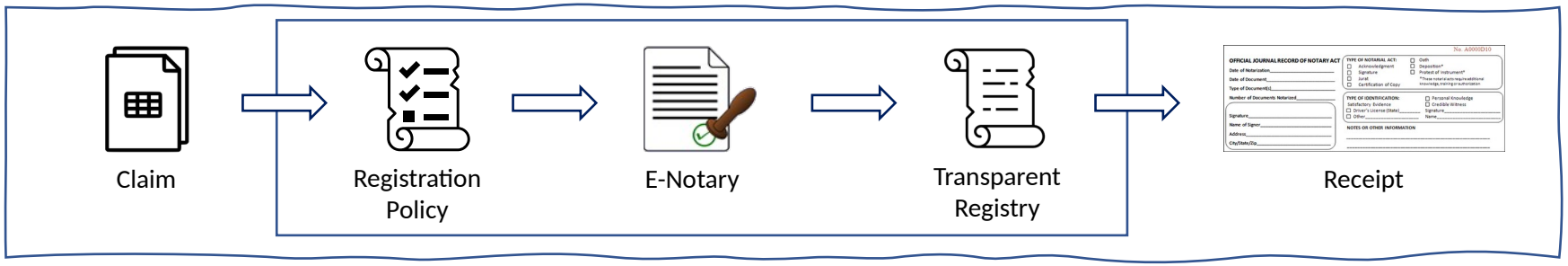
Many other vulnerabilities highlight the need for greater visibility into supply chain integrity, transparency, and trust to make an informed decision.

Use Case:

Software Supply Chain focusing on SBOM as evidence to a claim

Terms & Architecture

Definitions & Terms



Claim: An identifiable and non-repudiable statement about an artifact made by an Issuer

Registration Policy: Configuration for the types of identifiers representing issuers that may be verified, or rejected, by the notary before being placed on the registry

E-Notary: The act of verifying the identity of an issuer, submitting content to the system (storage + registry), based on policy, issuing a receipt for valid entry in a registry

Transparent Registry: A verifiable data structure that provides a consistent, append-only, record of all registered claims. Transparency does not *necessarily* mean public access; the notary may implement an access control policy.

Receipt: An offline, universally-verifiable proof that an entry is recorded in the registry. Receipts do not expire, but it is possible to append new entries that subsume older entries

https://ietf-scitt.github.io/draft-birkholz-scitt-architecture/draft-birkholz-scitt-architecture.html#name-definition-of-transparency

Transparency: Core Intuitions

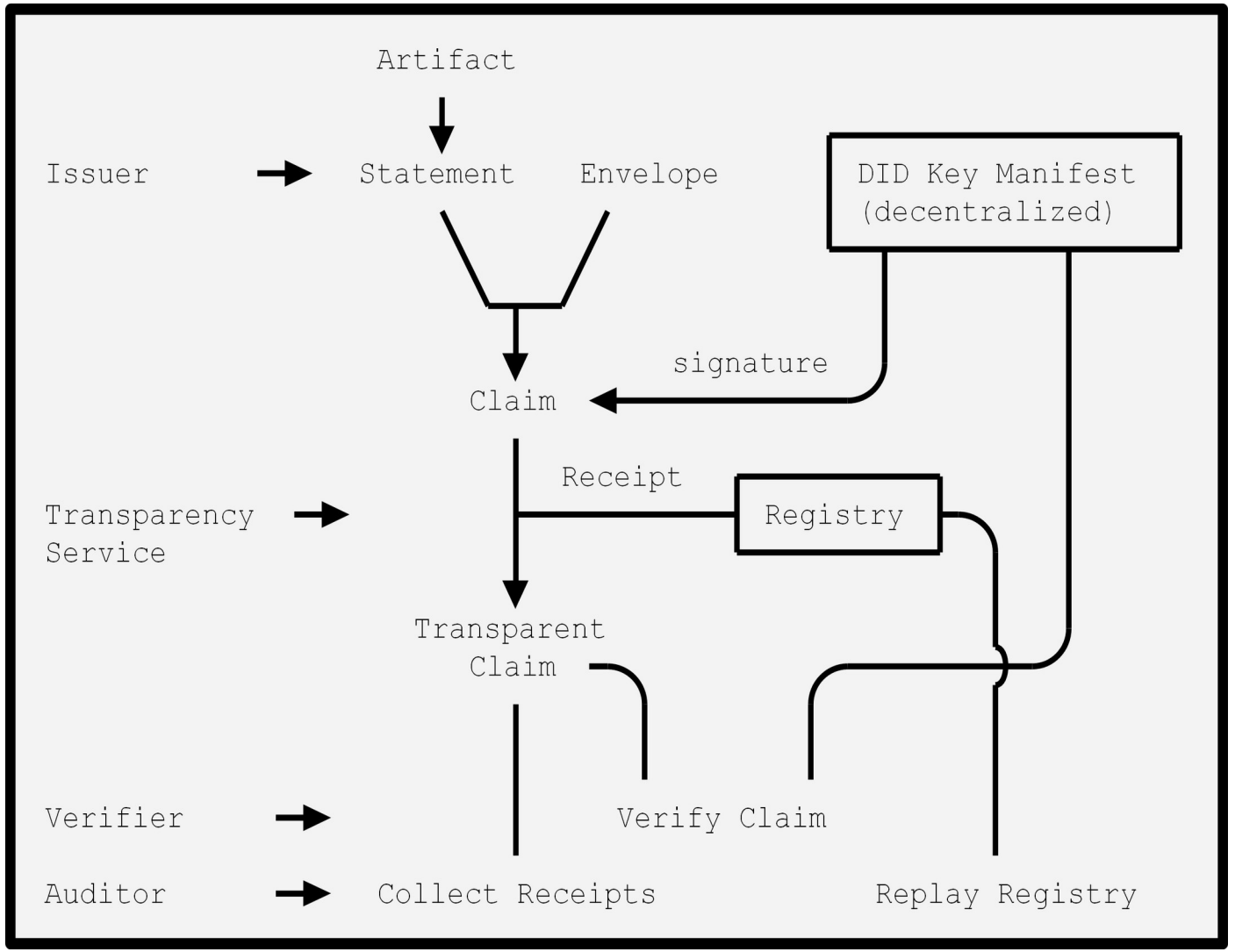
- We cannot stop authorized supply chain actors from making false claims, but we can make them accountable by requiring their claims to be registered in a verifiable and transparent data store.
- This ensures that malicious actors who make contradictory claims to different entities (customers, auditors, regulators) can be disambiguated from valid actors.
- All consumers of claims must first verify the proof of transparency registration to ensure a claim is auditable; this proof should be compact and fast to verify offline.

Transparency: Prior Work

Many examples are available. Here is a selection with many more are available:

- Certificate Transparency [RFC 9162] Adam Langley, Emilia Kasper, Ben Laurie (Google)
- CONIKS: bringing key transparency to end users , M. S. Melara, A. Blankstein, J. Bonneau, E. W. Felten, and M. J. Freedman (USENIX Security'15).
- Keeping authorities "honest or bust" based on large-scale decentralized witness cosigning (IEEE S&P '16)
- CHAINIAC: Proactive Software-Update Transparency via Collectively Signed Skipchains and Verified Builds (Usenix'17, EPFL)
- Contour: A practical system for binary transparency logging on bitcoin the latest authorized binary version.
  M. Al-Bassam, S. Meiklejohn (Data Privacy Management, Cryptocurrencies and Blockchain Technology, 2018).
- Confidential Consortium Framework (CCF)

Architecture



Milestones & Program of Work

Milestones

- Architecture and Terminology
- Information and Interaction Models
- Countersigning Format for Claim Registration
- HTTP-based REST API for Request-Response Interactions

Deliverables

- The main deliverables defined by this program of work provide a guideline for milestones that are in scope of the WG charter.
- Documents produced by the WG will address one or more of the following main deliverables:
  - Architectural Model: Actors, Interactions, Terminology
  - Consistent Actor Identification
  - Information Models and Interaction Models
  - Versatile Countersigning Format in Support of Transparency Services
  - Generic Protocol Bindings for Information Model and Interaction Models

Architectural Model

Actors, Interactions, Terminology

- The WG shall start out by documenting and defining terms in an architectural model for:
  - essential classes of actors such as the supply chain "issuer" (one which generates supply chain artifacts and statements about them) and
  - the basic interactions these have with other actors, and their duties in the ecosystem.
- The architectural model shall provide an aggregated overview of corresponding actor-specific information models and interaction models and will provide examples of composition patterns that illustrate how to address a concise set of use cases.

Consistent Actor Identification

- The WG shall select (and potentially profile) acceptable common identity format/formats that will be used to identify and authenticate actors in the SCITT ecosystem.

Information Models and Interaction Models

- **Registry**: The WG shall define an Abstract Transparent Registry that describes the interactions and conceptual messages that will and can be supported by registries to generate homogeneity across multiple supply chains.
- **Notarization**: The WG shall develop a specification that describes the notarization information model and the interaction model a notary will use to interact with supply chain entities.
- **Auditing**: The WG shall develop standards for auditing the supply chain claims that are introduced in the transparent registry. This will, in turn, generate audit claims based on an information model (results of the audit), which can be introduced in the same registry. A corresponding interaction model will describe how audit information can be queried by supply chain consumers (end customers) before making critical business decisions.

Versatile Countersigning Format

In Support of Transparency Services

- The WG shall specify standard formats for proofs of inclusion in the transparent registry.
- The standard shall enable independent verification of supply chain claims at a (much) later point on multiple platforms, and independent registration of claims in multiple registries.

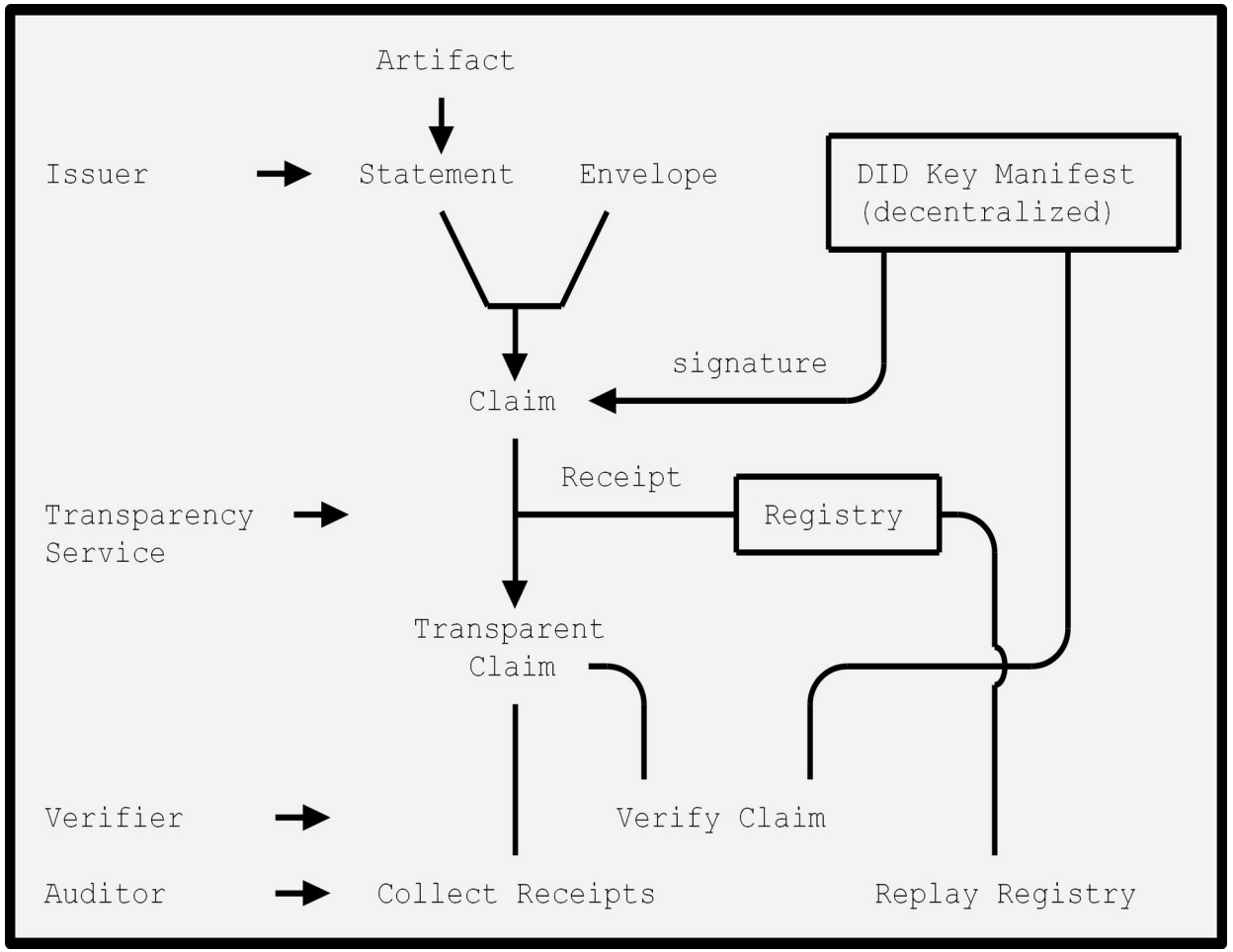
- WG will NOT develop new authentication and identity technologies

Generic Protocol Bindings
For Information Model and Interaction Models

- The WG shall standardize REST APIs and potentially other *existing* generic interaction schemes providing various actor interactions within the supply chain ecosystem
- Including standard inter-component message formats supporting reference implementations of SCITT building blocks for industry-wide interoperability

Discussion

Discussion Architecture



Milestones

- Architecture and Terminology
- Information and Interaction Models
- Countersigning Format for Claim Registration
- HTTP-based REST API for Request-Response Interactions

BoF Questions

- Do you think that the revised problem statement is clear?
- Can I see a show of hands of folk willing to review documents?
- Who would be willing to serve as an editor one of the listed documents?
- Do you think that given the charter revisions discussed on the mailing list and during the BOF (subject to review and finalization on the mailing list), a WG should be formed?
- How many people feel that a WG should not be formed?

Wrap-up and Conclusion

Material

- Mailing list: https://www.ietf.org/mailman/listinfo/scitt
- Charter: https://github.com/ietf-scitt/charter/blob/master/ietf-scitt-charter.md
- Drafts:
  - Countersigning COSE Envelopes in Transparency Services
  - An Architecture for Trustworthy and Transparent Digital Supply Chains